

**EXHIBIT A**

**Port Of Charleston Dirty Bomb Hoax and Social Media Liability**

**(30 pages)**

# **PORT OF CHARLESTON DIRTY BOMB HOAX AND SOCIAL MEDIA LIABILITY**

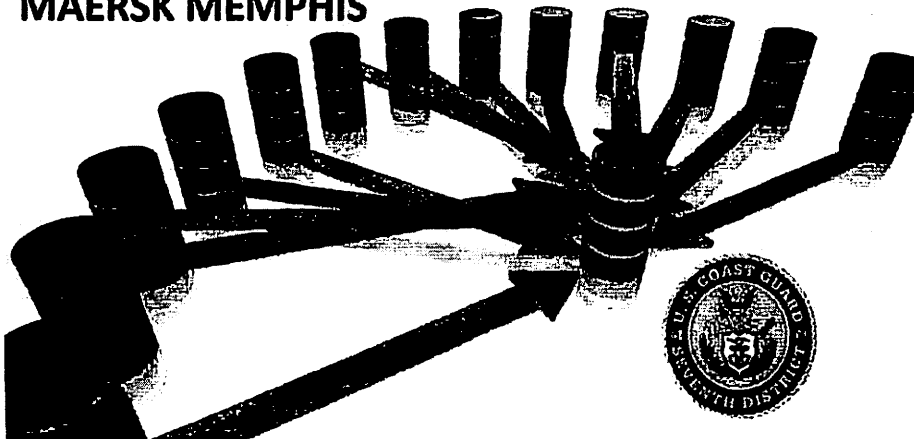
**“DIRTY BOMB ... PLEASE  
INVESTIGATE ... MAERSK MEMPHIS”**



## **Port of Charleston Dirty Bomb Hoax**

**Immediate Need for Deterrence  
Against Weaponized Deception**

**DIRTY BOMB ... PLEASE INVESTIGATE ...  
MAERSK MEMPHIS**



**WARNING:** This document provides a threat assessment of a cyber-attack vector. Individuals listed in this report should not be considered guilty of any crime or offense. The focus of this document is to present evidence of the telecommunications aspects of the "dirty bomb" alert and warning received by the U.S. Coast Guard on June 14<sup>th</sup>, 2017 in the context of federal law. Any individual discussed should be presumed innocent of any crimes until adjudicated otherwise in an appropriate court of law.



## ***Executive Summary***

This evidentiary report places certain actions of a YouTube celebrity, who initiated a radiological event response during a hoax reality news show, within the context of federal law.

As demonstrated by the Port of Charleston "dirty bomb hoax" on June 14<sup>th</sup>, 2017, profit-motivated YouTube entertainers masquerading as legitimate news channels are now an emerging threat to the critical infrastructure operators of the United States.

This dangerous trend indicates that socially engineered public panics can be used to mask more serious simultaneous cyber-attacks (known as blended attacks).

Blended critical infrastructure attacks can be composed of (1) hoax or false **content** designed to alarm and distress, and (2) are distributed devices designed to **flood and overwhelm** the target. The goal of a blended act is to force an ill-advised **call-to-action** (CTA) upon the victim.

This type of weaponized deception is the product of supposed "crowd sourcing". Crowd sourcing themes can drive Live Action Role Plays (**LARPs**) that offer an Augmented Reality Game (**ARG**) experience couched in the terms of "investigative journalism".

The journalism reality show **CrowdSourceTheTruth** (CSTT) operated by Jason Goodman, convinced two (2) audience members to call the duty officer at the U.S. Coast Guard Charleston Sector with verbal information about a "dirty bomb" which led to the closure of a marine terminal in June 2017.

**Three minutes** after the initial verbal reports were telephoned to the U.S. Coast Guard Charleston Sector, CSTT's Goodman asked his audience of over **2,000** to tweet the following message to 7<sup>th</sup> District U.S.C.G. Unified Command (resulting in a "**Twitter Storm**" of **8,000** impressions).

**"DIRTY BOMB ... PLEASE INVESTIGATE ... MAERSK MEMPHIS"**

The second warning ("Twitter Storm") was a distributed denial of service (**DDoS**) attack that transmitted false and deceptive information to an official U.S. Government law enforcement agency.

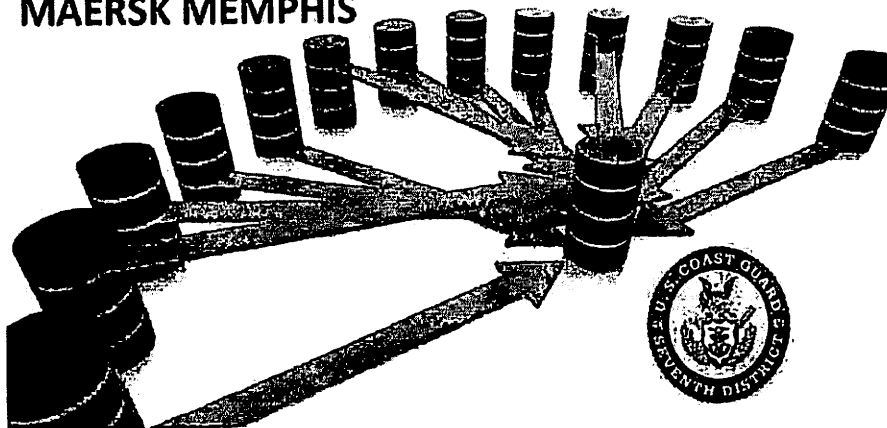
These activities appear to violate the following federal laws.

**18 U.S.C. 1038**      **CONTENT:** Goodman caused to be transmitted the following message to the 7<sup>th</sup> District Coast Guard Headquarters: "**DIRTY BOMB ... PLEASE INVESTIGATE ... MAERSK MEMPHIS**". This content was fake and a hoax.

**18 U.S.C. 1030**      **DELIVERY:** Goodman caused the above message to be transmitted with at least 8,000 Twitter impressions in a Distributed Denial of Service (**DDoS**) attack on the 7<sup>th</sup> District U.S. Coast Guard Headquarters (Unified Command).

As depicted below, the **content** of the message ("DIRTY BOMB etc") was based on false and deceptive information. The vehicle used to transmit the message to the U.S. Coast Guard 7<sup>th</sup> District Unified Command was a **DDoS-style** attack via Twitter.

**DIRTY BOMB ... PLEASE INVESTIGATE ...  
MAERSK MEMPHIS**

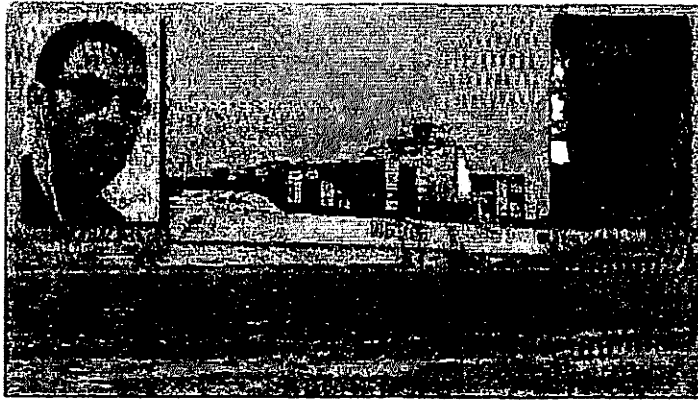


## Contents

<i>Executive Summary</i> .....	3
PART I: .....	6
<i>Background</i> .....	8
<i>Weaponized Deception</i> .....	9
<i>Weak Legal Deterrence Provides Immunity to Hoax Channels</i> .....	10
PART II: .....	11
<i>Overcoming the Legal Obstacles to Prosecution</i> .....	12
<i>The Curious Deep Uranium, aka Rock Hudson of The Hudson Report</i> .....	14
PART III: .....	16
<i>Presumed Violations of Federal law</i> .....	17
PART IV: .....	19
<i>Weaponization of Attack Bots by CSTT Affiliates</i> .....	20
<i>Attack Tools Border on Cyber Warfare</i> .....	22

**PART I:**  
**HOAX THREAT ACTORS**  
**ATTACK U.S.C.G.**  
**7<sup>th</sup> DISTRICT**



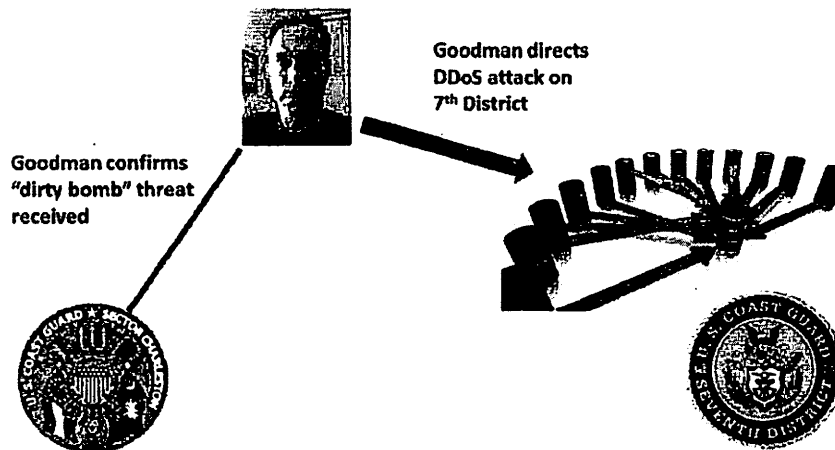


L/R: Jason David Goodman, the MAERSK MEMPHIS, George Webb Sweigert

### Three minutes between incident A and incident B

2:01:28

2:04:28



Taxonomy of distribution of dirty bomb alert and warning.

### **Background**

No individual(s) have ever been held accountable for the social media generated public hysteria that led to the emergency closure of a marine terminal at the Port of Charleston, S.C. on June 14<sup>th</sup>, 2017.

The maritime terminal closure was based on a "dirty bomb" tip provided by individuals that supposedly had knowledge of the shipment of a weapon of mass destruction (WMD) on the **MAERSK MEMPHIS** container ship (arriving in the Port of Charleston).

Two separate incidents of "dirty bomb" warnings occurred in sequence.

#### **Incident A**

Two (2) "dirty bomb" phone calls were received by the U.S. Coast Guard (U.S.C.G.) duty officer at the Charleston Sector after CSTT "intelligence coordinator" Goodman provided the emergency number live on the air (**843-740-7050**)<sup>1</sup>.

At least one of these callers was discovered to be a very close affiliate of the CSTT reality show (allegedly **Joe Napolitano**).

A third call was made to the duty officer by Goodman himself to confirm that the "dirty bomb" messages were received.

Goodman (during a third call) verified (live on-air) with the duty officer at the Charleston Sector that U.S. Coast Guard Charleston Sector<sup>2</sup> that he had received the "dirty bomb" warnings.

### **THREE MINUTES TRANSPIRE**

#### **Incident B**

Three minutes after Goodman's call to the Charleston Sector Goodman orchestrated a **DDoS** attack by suggesting everyone in his 2,117 member audience send a Twitter message to the higher command of the Charleston Sector – 7<sup>th</sup> District Unified Command. The transmission of these tweets resulted in 8,000 Twitter impressions, which flooded the 7<sup>th</sup> District with the following message.

#### **"DIRTY BOMB – PLEASE INVESTIGATE – MAERSK MEMPHIS"**

There appears to be no legitimate reason to justify the redundant DDoS "Twitter Storm". Understandably, these messages created a panic that bordered on mass hysteria accompanied by a full-scale radiological incident response followed requiring the deployment of police, fire, EMS, public works, specialty teams, etc.

---

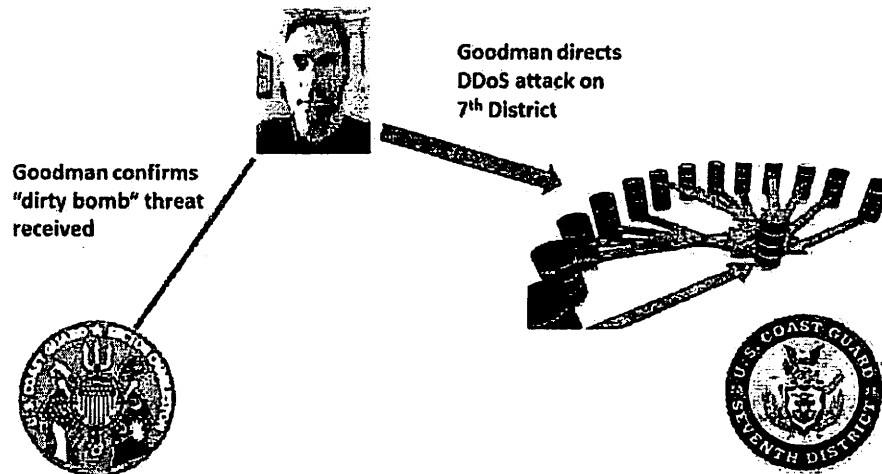
<sup>1</sup> <https://www.nytimes.com/2017/06/15/us/port-dirty-bomb-south-carolina.html>

<sup>2</sup> <https://www.atlanticarea.uscg.mil/Our-Organization/District-7/Units/Sector-Charleston/>

### Three minutes between incident A and incident B

2:01:28

2:04:28



#### ***Weaponized Deception***

For Internet celebrities willing to create hoaxes based upon deceptive information (labeled as "news") their drama can be wrapped in an "investigative journalist" wrapper. This enables such channels to be in the center of the news, rather than merely just report the news.

CSTT hoaxes usually involve the activation of public safety resources to increase the allure of the perceived threat for the audience. This creates a strong emotional bond between the audience, actors and the storyline.

After audience members develop emotional commitment and engagement, a CSTT call-to-action (CTAs) is coerced from them. These CTAs may include e-mail bombing a target's mail address, calling the places of employment of targets and reporting criminal investigations, inciting acts of retribution against targets perceived as "enemies of the truth", etc.

Theatrical presentations of "nerve centers" (like CSTT) can bring an audience to an enhanced climax based on the inducement of fear. This can be likened to the Orson Wells broadcast of "War of the Worlds" in 1938. Such reality shows, also known as Live Action Role Plays (LARP), include the injection of periodic "intelligence reports" from "inside sources" to create an Augmented Reality Game (ARG).

These same threat actors (CSTT + CSTT affiliates) have recently increased their threat capability by operationalizing technical "attack bots" designed to automatically broadcast false information when a certain set of circumstances triggers their logic. These bots can be deployed to create "Twitter Storms" similar to Charleston.

CSTT threat actors have openly stated their desire to attack critical infrastructure to "crash the machine" and "reset the system" as part of an Internet doomsday cult philosophy<sup>3</sup>. Operationalized attack auto-bots factor heavily into this philosophy. This is not a fanciful and harmless threat.

The lack of criminal prosecution of these threat actors has created a fertile environment for continued testing and prototyping of these hoax enhancing auto-bots.

### ***Weak Legal Deterrence Provides Immunity to Hoax Channels***

Laws and policies only deter if three conditions are present:

- Fear of penalty
- Probability of being caught
- Probability of penalty being administered

No deterrence has been undertaken to mitigate these CSTT hoax threat actors from creating more hoaxes impacting public safety. Since Charleston copy-cat hoax events have been staged in New Mexico by the same profit-driven threat actors (claiming an assassination attempt made on a CSTT "reporter").

These repeated public safety hoaxes appear to be an act of perfecting their hoax attack methods. There is a definite and well documented life cycle to the hoaxes created by "CSTT" to generate views and profits.

This type of threat to critical infrastructure has yet to be addressed firmly with legal action. Thus, a deterrence capability is lacking. Without effective deterrence, others (motivated by profit) will stage similar hoaxes.

---

<sup>3</sup> See #TeamTyler and Project Mayhem operated by Quinn Michaels

**PART II:**  
**WILLFUL BLINDNESS OF CSTT**

### ***Overcoming the Legal Obstacles to Prosecution***

CSTT hoax threat actors are fond of relying on their willful blindness and conscious disregard to apparent common sense, facts and contradictory information as an immunity defense.

The consistent reliance on ignorance to certain facts is an example of willful recklessness to avoid the truth. CSTT affiliates deliberately feign ignorance and practice avoidance of the actual circumstances surrounding these hoax events.

#### **Willful blindness in a criminal context**

**Example:** When a drug transport smuggler ("mule") crosses the U.S.-Mexican border they can claim s/he was not aware of the 162 pounds of marijuana in the car's secret compartment. This willful ignorance defense does not work.

In the same manner, when profit-motivated hoax threat actors forwards unvented warnings ("dirty bomb") to law enforcement<sup>4</sup> (understanding the consequences of such information) and then claims ignorance of the consequences ("I trusted the source") it represents a fact pattern as described in United States v. Jewell, 532 F.2d 697 (9th Cir. 1976):

*"One with a deliberate antisocial purpose in mind . . . may deliberately 'shut his eyes' to avoid knowing what would otherwise be obvious to view. In such cases, so far as criminal law is concerned, the person acts at his peril in this regard, and is treated as having 'knowledge' of the facts as they are ultimately discovered to be."<sup>5</sup>*

Goodman's own words demonstrate the concept. In the following show excerpt, Mr. Goodman speaks about the trust he has placed in someone called "Deep Uranium" (later discovered to be a former FBI informant) as source the "dirty bomb" warnings.

Recall **Incident A** when Mr. Goodman verified via phone call that the duty officer at the U.S.C.G. Sector Charleston had received a "dirty bomb" threat. Then the following remarks are made by Goodman on video, immediately following confirmation of the "dirty bomb" warning.

---

<sup>4</sup> <https://law.justia.com/cases/federal/appellate-courts/F2/532/697/99156/>

<sup>5</sup> R. Perkins, Criminal Law 776 (2d ed. 1969)

*"...We've received information from a person known to me through George (Webb) as someone who is in the law-enforcement community or the whatever intelligence community. I don't know this person but I know that George frequently tells me he's spoken to this person . . . George tells me he's spoken to this person and such and is going to happen and then ... more than once the person was correct."* 2:30:20 of video<sup>6</sup>. Remarks of Jason Goodman on 6/14/2017 YouTube reality show "CSTT".

Recall **Incident B** when Mr. Goodman requested **2,117** audience members tweet "DIRTY BOMB – PLEASE INVESTIGATE – MAERSK MEMPHIS" to the 7<sup>th</sup> District Unified Command (resulting in 8,000 Twitter impressions).

However, an hour prior to these events Goodman telephone intelligence analyst and author Dr. Jermon Corsi<sup>7</sup> to seek his advice and consultation.

**01:09:42** Jason Goodman contacts Corsi to inquire about the threat

**01:17:15** Corsi responds he doesn't know anything about the threat

**01:20:51** Corsi re-iterates he cannot corroborate anything about the threat

**01:41:06** Corsi repeats again he has ZERO confirmation of the threat



Clear and Present Danger (Calm Before the Storm?) #maerskmemphis

Video of CSTT, Jason Goodman owner/operator

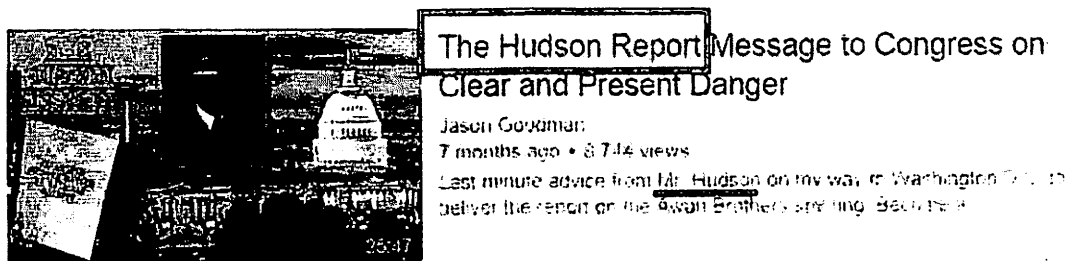
<sup>6</sup> <https://www.youtube.com/watch?v=ekr5cw2WAbU&t=7799s>

<sup>7</sup> <http://www.simonandschuster.com/authors/Jerome-R-Corsi/48217651>

This information from an intelligence industry analyst and "insider" was subsequently disregarded by Goodman.

In sum, Mr. Goodman proceeded at his own peril and risk to broadcast the fake hoax threat to the 7<sup>th</sup> District Unified Command (**Incident B**) based on vague and ambiguous knowledge of a mystery man known as "Deep Uranium".

The source of this dirty bomb "intelligence" ("Deep Uranium") is a former FBI informant. It is very telling that a few weeks after the 6/14/2017 Port of Charleston incident, Mr. Goodman inaugurated a special CSTT exclusive weekly feature known as the **Hudson Report** featuring "Deep Uranium" on August 14, 2017.



Screen capture of The Hudson Report

### ***The Curious Deep Uranium, aka Rock Hudson of The Hudson Report***

The identity of the curious "Deep Uranium" appears to be that of a former FBI informant living in West Virginia.



Man On Mission To Restore Fletcher Church

The likely individual known as Deep Uranium and Rock Hudson on CSTT<sup>8</sup>

<sup>8</sup> <https://www.youtube.com/watch?v=zpSZ-NC8ils>



## **Militia leader guilty in bomb plot**

**Aug. 8, 1997**

**WHEELING, W.Va.** -- The self-proclaimed general of West Virginia's Mountaineer Militia has been convicted of plotting to blow up the FBI's fingerprint laboratory. A U.S. District Court jury found Floyd 'Ray' Looker, a Vietnam veteran who lives in Stonewood, W.Va. and claims to be a gospel preacher, guilty of conspiracy to engage in manufacturing and dealing in explosives without a license.

The 56-year-old Looker, who testified in his own behalf Thursday, had told jurors he didn't know it was illegal to build bombs. He said he wanted to stockpile explosives in case the United States were invaded by a foreign force. The government, however, said Looker planned to use the explosives to blow up the FBI's fingerprint lab in Clarksville, W.Va., about 90 miles south of Pittsburgh. Looker was arrested Oct. 11, 1995 after he allegedly sold blueprints of the FBI fingerprint complex for \$50,000 to an undercover agent who claimed to represent a terrorist group. The prosecution's case was based information received from a former militia member who has since entered the government's witness protection program. The informant, **Okey**

**Marshall Richards Jr.**, made more than 400 tape recordings that led to the arrest of Richards. Defense attorneys called Richards' two ex-wives who told the court the informant is a pathological liar. The two women also said he owed them at least \$40,000 in alimony and child support. Looker's co-defendants, Jack Arland Phillips and Edward F. Moore, both entered guilty pleas at earlier hearings.

The Hudson Report was marketed by CSTT as an "intelligence report", including a synopsis of leaked law-enforcement and/or intelligence community information. The focus of The Hudson Report was to create drama and interest based on upcoming events related to "intelligence assessments".

This was a regular feature of CSTT; the showcasing of the same individual who was the alleged source of the "dirty bomb" threat information.

**PART III:  
SUFFICIENCY OF  
LEGAL REMEDIES**

### ***Presumed Violations of Federal law***

#### **18 U.S.C. § 1030, COMPUTER FRAUD AND ABUSE ACT**

18 U.S.C. § 1038 states:

- (5)  
(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

In 2011, the Sixth Circuit Court of Appeals addressed similar DDOS-style attacks in *Pulte Homes, Inc. v. Laborers' Intern. Union of North America*, 648 F.3d 295 (6th Cir. 2011).

This case that did not deal directly with a per se DDOS attack but did deal with a labor union's concerted email and telephone "attack" on a company of such a volume that it disrupted the company's ability to do business<sup>9</sup>.

The issue before the court in *Plute* was whether the labor union "intentionally caused damage" by causing e-mail bombs and needless phone calls to a business. The Pulte Court, in finding a violation of the Computer Fraud and Abuse Act and, consequentially, "damage" arising from this activity, held that "a transmission that weakens a sound computer system—or, similarly, one that diminishes a plaintiff's ability to use data or a system" causes damage. *Id.* at 301. The court reasoned:

Under the CFAA, "any impairment to the integrity or availability of data, a program, a system, or information" qualifies as "damage." Because the statute includes no definition of three key terms—"impairment," "integrity," and "availability"—we look to the ordinary meaning of these words. "Impairment" means a "deterioration" or an "injurious lessening or weakening." The definition of "integrity" includes an "uncorrupted condition," an "original perfect state," and "soundness." And "availability" is the "capability of being employed or made use of." Applying these ordinary usages, we conclude that a transmission that weakens a sound computer system—or, similarly, one that diminishes a Plaintiff's ability to use data or a system—causes damage."

---

<sup>9</sup> <https://shawnetuma.com/2013/10/09/yes-case-law-says-it-really-is-a-cfaa-violation-to-ddos-a-website/>

**18 U.S.C. § 1038, TERRORIST HOAX IMPROVEMENTS ACT OF 2007**

18 U.S.C. § 1038 states:

**(a) Criminal Violation.—**

**(1) In general.—Whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of [specified anti-terrorism laws,] shall [be fined or imprisoned as provided].**

In 2017, a 21 y.o. volunteer fire fighter in Columbia, S.C. was sentenced to one year of imprisonment and three years of supervised probation for phone texting three unknown people that he had heard that someone placed a bomb at a Veteran's Administration Medical Center<sup>1</sup>.

As suggested in *United States v. Jewell*, 532 F.2d 697 (9th Cir. 1976), Mr. Goodman's willful blindness to the sources of the 6/14/2017 dirty bomb warnings (calculated to cause panic and disrupt the civil peace) does not provide an adequate defense.

To address the intent requirement of 18 U.S.C. 1038 it is instructive to note the wisdom of *United States v. Castagana*, 604 F.3d 1160, 1164 (9th Cir. 2010).

*Whether the circumstances were such that Castagana's victims or other observers may reasonably have believed his statements to indicate terrorist activity is a question wholly independent of Castagana's intentions. That is precisely what a reasonableness standard, triggered by factual circumstances, means. The insertion of this reasonableness requirement removes from consideration the subjectivity of the actor's intent and replaces it with an objective standard.*

The intention of Mr. Goodman is not an issue. The willful blindness on Goodman's part to seize on "intelligence" information from a former FBI informant to create a Twitter Storm is the issue.

**PART IV:  
BURGEONING CAPABILITIES  
OF  
CSTT THREAT ACTORS**

### ***Weaponization of Attack Bots by CSTT Affiliates***

Cognitive (mind) threats are a type of social engineering attack that demands immediate action based on a perceived crisis (always based on deception). For such attacks to work there must be an appearance of legitimacy ("intelligence source"). E-mail phishing attacks are an example of deception based social engineering designed for an illegitimate call to action.

These attacks (like **Incident B**) can overwhelm public safety responders in an instant, sewing confusion which blurs proper situational awareness and threat assessment.

The speed of the Internet, the large audience reach of social media platforms, and the opportunity to fashion hoax events create attacks that are largely unknown and unfamiliar to public safety responders.

Deception coupled with "auto bot" or "bot" technology is even more troubling. The same CSTT group responsible for Charleston is perfecting a type of "doomsday" auto-bot messaging system with the end objective to "reset the machine".

These CSTT affiliates (emboldened by the lack of a legal threat) are openly communicating via YouTube and Twitter to create a Project Mayhem type of doomsday network. This is a recipe for a larger scale hoax in the future.

The auto-bot network can (labeled #TimePhoneHack) disseminate massive disinformation via social media networks to create panic in seconds. The same CSTT threat actors involved in Charleston are now using sophisticated Artificial Intelligence (AI) techniques to perfect their methods (in plain view).

### Time Phone Hack #tyler #teamtyler - YouTube



<https://www.youtube.com/watch?v=Q5B6OZInPTU>

4 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ..

### Time Phone Hack #Tyler #TeamTyler - YouTube

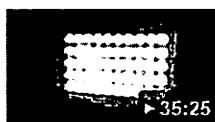


<https://www.youtube.com/watch?v=3jy8xc02aH8>

4 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ..

### Time Phone Hack How To Hack Time - YouTube



<https://www.youtube.com/watch?v=n4e481lAsbo>

1 day ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ..

### Time Phone Hack And Were Back - YouTube

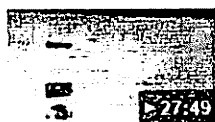


[https://www.youtube.com/watch?v=LvSi7-ab\\_Sk](https://www.youtube.com/watch?v=LvSi7-ab_Sk)

1 day ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ..

### Time Phone Hack More Entertaining - YouTube



<https://www.youtube.com/watch?v=ZNVJ56T8Ktk>

2 days ago - Uploaded by quinn michaels

Developing artificial intelligence with a unique perspective. Quinn Michaels is working on Indra.ai an artificial ..

### ***Attack Tools Border on Cyber Warfare***

Cognitive attacks (weaponized deception) coupled with technology devices (auto-bots) have created a new style of cyber threat known as blended attacks. Such attacks are multi-layered and can avoid traditional pre-attack indicators. Techniques such as these are bordering on the domain of cyber warfare.

The sophistication of this style of attack will remain perplexing to traditional first responder resources (as with Charleston). As this paper is being written, a bot-net style attack apparently launched by CSTT is presently underway.

The CSTT affiliate known as "Quinn Michaels" is presently openly recruiting followers to launch cyber-based attacks in the perceived enemies and rivals of CSTT. Michaels, who claims to understand the Palantir<sup>10</sup> intelligence algorithms, is engineering an Artificial Intelligence (A.I.)-based bot network to monitor social media for trigger words and respond with replies to guide and enhance a cognitive attack.

These attacks indicate that the CSTT confederation have not been deterred by the closure of the Port of Charleston and the downstream consequences of that event. In fact, the opposite is true – they have become embolden by the lack of legal accountability.

This type of threat to critical infrastructure has yet to be addressed firmly with legal action. Thus, a deterrence capability is lacking. Without effective deterrence, others (motivated by profit, philosophy, ideologies, etc.) with stage similar hoaxes.

Meanwhile, the lack of criminal prosecution of these threat actors has created a fertile environment for testing and prototyping hoax enhancing auto-bots.

---

<sup>10</sup> <https://www.bloomberg.com/features/2018-palantir-peter-thiel/>




## **ANNEX**

**Dr. Jermone Corsi (consulted one hour before Incident B)**

File Edit View Favorites Tools Help

Not logged in Talk Contributions Create account Log


**WIKIPEDIA**  
The Free Encyclopedia

Article Talk

Read Edit View history Search Wikipedia

Main page  
Contents  
Featured content  
Current events  
Random article  
Donate to Wikipedia  
Wikipedia store  
Interaction  
Help  
About Wikipedia  
Community portal  
Recent changes  
Contact page  
Tools  
What links here  
Related changes  
Upload file  
Special pages  
Permanent link  
Page information  
Wikidata item  
Cite this page  
Print/export  
Create a book  
Download as PDF  
Printable version  
In other projects  
Wikiquote

## Jerome Corsi

From Wikipedia, the free encyclopedia

**Jerome Robert Corsi** (born August 31, 1946) is an American author, political commentator, and conspiracy theorist.<sup>[a]</sup> best known for his two *New York Times* Best Selling books: *The Obama Nation* and *Unfit for Command* (with co-author John O'Neill). Both books, the former written in 2008 and the latter in 2004, attacked Democratic presidential candidates and were criticized for including numerous inaccuracies.<sup>[b][c]</sup>

In other books and columns for conservative sites such as *WorldNetDaily* and *Human Events*, Corsi has discussed topics that are considered conspiracy theories, such as the alleged plans for a North American Government, the theory that President Barack Obama is not a United States citizen,<sup>[a]</sup> criticism of the United States government for allegedly covering up information about the terrorist attacks of September 11, 2001,<sup>[d]</sup> and alleged United States support of Iran in its attempts to develop nuclear weapons.<sup>[10][11][12]</sup>


In 2017, he became the Washington, D C bureau chief for the conspiracy theory website *InfoWars*.

### Contents

1 Early life and education
2 Career
3 Writings and conspiracy theories

3.1 *Unfit for Command*
3.2 *The Obama Nation*
3.3 *Black Gold Stranglehold*
3.4 *Atomic Iran*
3.5 *Where's the Birth Certificate?*

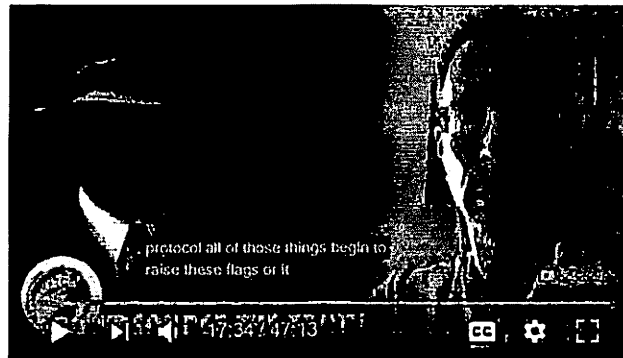
### Jerome Corsi



**Corsi in 2018**

<b>Born</b>	Jerome Robert Corsi August 31, 1946 (age 71) East Cleveland, Ohio, U.S.
<b>Residence</b>	Denville Township, New Jersey, U.S.
<b>Nationality</b>	American
<b>Education</b>	Case Western Reserve University (BA) Harvard University (PhD) [1]
<b>Occupation</b>	Writer
<b>Employer</b>	InfoWars[2]
<b>Known for</b>	Co-author of <i>Unfit for Command</i> , author of <i>The Obama Nation</i>
<b>Title</b>	DC bureau chief[2]
<b>Political</b>	Constitution Party

**“Rock Hudson” discusses the Port of Charleston in an August 14, 2017 video<sup>11</sup>.**



**Hudson Revealed**



Jason Goodman



19,801 views



Published on Aug 14, 2017

***"In regards to **George Webb** I have a tremendous respect for Webb and I don't mind telling you –***

***and that is that **George is just an amazing** – that you what a mind -- yeah – what a mind – I can't speak enough of it, I mean it's just ....***

***You take for example intelligence and people say well how do we know this guy [Hudson] is telling us the truth – well okay ...***

***We know, we know for a fact that **425 million cargo containers** are transported each year in the world that represents over 90 percent of the world's total trade ...***

***Charleston South Carolina is a port hub – those hubs – depending on the security protocols that their using – that day or that shift – they can process 1,500 to **50 thousand** containers per day. That raised an eyebrow with me...***

***But, don't worry because they really do care about you ...***

***They should be ashamed of themselves ..."** Beginning at 39:20 in the YouTube video "Hudson Revealed" published August 14, 2017.*

---

<sup>11</sup> <https://www.youtube.com/watch?v=TWUI8gDPF0&t=2021s>

**Goodman provides recap of the dirty bomb hoax at 1:33, names Joe Napoli at 3:13, continues on to 8:51**



Unrig Cynthia McKinney



Jason Goodman



0:00

11,504 views

[https://www.youtube.com/watch?v=tSl0ZflsN\\_k](https://www.youtube.com/watch?v=tSl0ZflsN_k)

**Example of the weekly "The Hudson Report" YouTube shows**



**Hudson Report - Benjamin Paddock & Battlefield Las Vegas**

Jason Goodman  
5 months ago • 23,870 views

Become a sponsor of Crowdsource the Truth and support the effort  
<http://paypal.me/crowdsourcethetruth> <https://www.patreon.com/>



**Hudson Revealed**

Jason Goodman  
6 months ago • 19,763 views

With over 40 years of military, intelligence and clandestine experience  
confidential Crowdsourc operative codename HUDSON



**The Hudson Report - Multiple Shooters in Las Vegas?**

Jason Goodman  
6 months ago • 16,933 views

Mr. Hudson provides his analysis that indicates multiple shooters, multiple rates of fire and multiple caliber weapons. Become a



**Hudson Report Awan Bros IT Scandal Hearing**

Jason Goodman  
6 months ago • 10,510 views

Mr. Hudson returns after being off grid for several days on a recon mission. He weighs in on the Las Vegas massacer Tom Fitton's



**Hudson Report - Criminal Congress**

Jason Goodman  
6 months ago • 5,960 views

Mr. Hudson continues to name names in the time and manner of his choosing as he enumerates a stunning historical list of

---

<sup>1</sup> <https://www.justice.gov/usao-sc/pr/columbia-man-sentenced-making-hoax-bomb-threat>



71911657R00018

Made in the USA  
Middletown, DE  
01 May 2018

The next generation of cyber warfare attack tools will be based upon Artificial Intelligence. A.I. tools can execute complex social media attacks to create panic. Law enforcement is falling further behind the tip of the spear in comprehending the cyber warfare nature of these attack techniques.

This booklet describes how social media hoax news sites can attack America's critical infrastructure. Seemingly, these deception merchants operate with no threat of legal action. This fertile environment has allowed the consequence-free attacks on maritime ports, generation of hysteria of supposed assassination plots, etc.

The alleged deception merchant described herein is Jason David Goodman of New York City, operator of the "business" CrowdSourceTheTruth (a social media conspiracy channel).

**WARNING:** No individuals described herein should be presumed to be guilty of any particular violation of law, policy or regulation. All parties should be presumed innocent until a competent court deems otherwise.

ISBN 9781717058795



9 781717 056795

90000 >

